## THE UNITED STATES DISTRICT COURT
## NORTHERN DISTRICT OF ILLINOIS, EASTERN DIVISION

| | | |
|---|---|---|
| EMAD KASHKEESH, BEAU ZANCA, | ) | |
| and MICHAEL KOMORSKI, individually | ) | Case No. 21-cv-03229 |
| and on behalf of a class of | ) | |
| similarly situated individuals, | ) | |
| | ) | |
| *Plaintiffs*, | ) | |
| | ) | |
| v. | ) | Hon. Gary Feinerman |
| | ) | |
| MICROSOFT CORPORATION, a | ) | Magistrate Hon. Heather K. McShain |
| Washington Corporation. | ) | |

## FIRST AMENDED CLASS ACTION COMPLAINT

Plaintiffs Emad Kashkeesh, Beau Zanca, and Michael Komorski ("Plaintiffs"), individually and on behalf of other similarly situated individuals, bring this Amended Class Action Complaint against Defendant Microsoft Corporation ("Defendant" or "Microsoft") for its violations of the Illinois Biometric Information Privacy Act, 740 ILCS 14/1, *et seq.* ("BIPA") and to obtain redress for all persons injured by Defendant's conduct. Plaintiffs allege the following based on personal knowledge as to their own acts and experiences, and as to all other matters, upon information and belief, including an investigation conducted by their attorneys.

## INTRODUCTION

1. Plaintiffs seek to represent a class of individuals who were drivers for the ridesharing and food delivery company Uber and had their unique facial biometrics collected and used without their consent or authorization by Microsoft when they interacted with the Uber mobile application to verify their identity.

2. On behalf of themselves and the proposed Class defined below, Plaintiffs seek an injunction requiring Defendant to comply with BIPA, as well as an award of statutory damages to the Class, together with costs and reasonable attorneys' fees.

## PARTIES

3. Plaintiff Emad Kashkeesh is a resident of Illinois.

4. Plaintiff Beau Zanca is a resident of Colorado.

5. Plaintiff Michael Komorski is a resident of Illinois

6. Defendant Microsoft Corporation is a Washington corporation that conducts, and is licensed by the Illinois Secretary of State to conduct, business throughout Illinois, including in Cook County, Illinois.

## JURISDICTION AND VENUE

7. This Court has subject matter jurisdiction over this matter pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d) et seq., because this case is a class action in which the matter in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs; there are greater than 100 putative class members; at least one putative class member is a citizen of a state other than Defendant; and none of the exceptions under subsection § 1332(d) apply.

8. This Court may assert personal jurisdiction over Defendant, because Defendant does business within Illinois and transacts business in Illinois such that it has sufficient minimum contacts with Illinois and/or has purposely availed itself of Illinois markets to make it reasonable for this Court to exercise jurisdiction over Defendant, and because Plaintiffs' claims arise out of Defendant's in-state actions as Plaintiffs' facial biometrics were knowingly obtained by Defendant in this District.

9. Venue is proper in this District because Plaintiffs reside in this District and a substantial part of the events giving rise to Plaintiffs' claims occurred in this District.

## THE BIOMETRIC INFORMATION PRIVACY ACT

10. “Biometrics” refers to a “biology-based set[s] of measurements.” *Rivera v. Google Inc.*, 238 F. Supp. 3d 1088, 1094 (N.D. Ill. 2017). Specifically, “biometrics” are “a set of measurements of a specified physical component (eye, finger, voice, hand, face).” *Id.* at 1296.

11. BIPA was enacted in 2008 in order to safeguard individuals’ biometrics as the result of the “very serious need [for] protections for the citizens of Illinois when it [comes to their] biometric information.” Illinois House Transcript, 2008 Reg. Sess. No. 276. BIPA is codified as Act 14 in Chapter 740 of the Illinois Compiled Statutes.

12. As set forth in BIPA, biologically unique identifiers, such as a person’s unique facial geometry, cannot be changed. 740 ILCS 14/5(c).

13. As a result of the need for enhanced protection of biometrics, BIPA imposes various requirements on private entities that collect or maintain individuals’ biometrics, including facial scans.

14. Among other things, BIPA seeks to regulate “the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information.” 740 ILCS 14/5(g). BIPA thus applies to entities that interact with two forms of Biometric Data: biometric “identifiers” and biometric “information.” 740 ILCS 14/15(a)-(e).

15. BIPA defines a “biometric identifier” as any personal feature that is unique to an individual, including fingerprints, voiceprints, palm scans and facial geometry. “Biometric identifiers” are physiological, as opposed to behavioral, characteristics. BIPA’s text provides a non-exclusive list of protected “biometric identifiers,” including “a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry.” 740 ILCS 14/10.

16. "Biometric information" is defined by BIPA as "any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual." *Id*. This definition helps ensure that information based on a biometric identifier that can be used to identify a person is covered by BIPA. Collectively, biometric identifies and biometric information are known as "biometrics."

17. In BIPA, the Illinois General Assembly identified four distinct activities that may subject private entities to liability:

a. possessing biometrics without a proper policy publicly available, 740 ILCS 14/15(a);

b. collecting biometrics, 740 ILCS 14/15(b);

c. profiting from biometrics, 740 ILCS 14/15(c); and

d. disclosing biometrics, 740 ILCS 14/15(d).

18. As the Illinois Supreme Court has held, BIPA "codified that individuals possess a right to privacy in and control over their biometric identifiers and biometric information." *Rosenbach v. Six Flags Entm't Corp*., 2019 IL 123186, ¶ 33, 129 N.E.3d 1197, 1206 (Ill. 2019). The Illinois Supreme Court further held that when a private entity fails to comply with BIPA "that violation constitutes an invasion, impairment, or denial of the statutory rights of any person or customer whose biometric identifier or biometric information is subject to the breach." *Id.*

## **FACTUAL BACKGROUND**

19. In an effort to provide its customers biometric authentication services, Defendant Microsoft Corporation developed a software known as the Face Application Programming Interface (or "Face API").

20. Defendant's Face API software is incorporated into its customers' mobile or internet-based applications and operates by collecting and analyzing individuals' facial biometrics as needed by Defendant's customers.

21. One of the most well-known and largest users of Defendant's Face API technology is Uber Technologies Inc. ("Uber"). Uber is one of the biggest ride-share companies in the world, connecting thousands of riders with its drivers through its mobile Uber application.

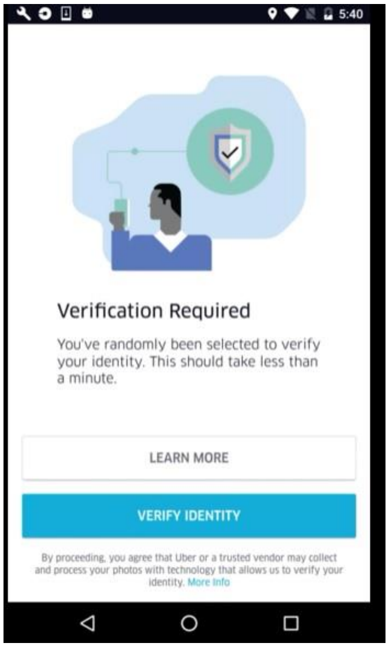
22. In addition, Uber has also leveraged its ride-share application to provide food delivery services through its driver network to thousands of customers through its mobile Uber Eats application.

23. Since 2016 Defendant's Face API software was utilized to periodically verify the identity of Uber drivers, including drivers operating in Illinois, by extracting and comparing drivers' unique biometric facial geometry templates.[1]

24. Specifically, Defendant's Face API was integrated into Uber's mobile phone application as part of Uber's security feature "Real Time ID Check." Upon registering to become an Uber driver, Plaintiffs and the other Class members were required to enter certain identifying information including, but not limited to, their full name, vehicle information, and driver's license, into the Uber application. Critically, Uber drivers are also required to provide a profile picture featuring their face by either taking a picture or providing a picture from their driver's license.

[1] https://customers.microsoft.com/en-us/story/731196-uber (last accessed July 29, 2021).

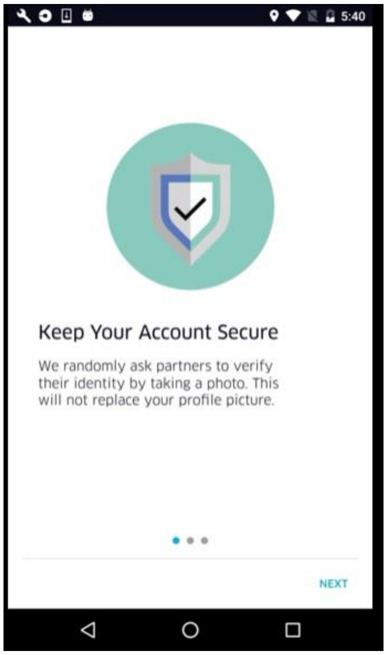
25. As shown in the series of pictures below that depict the verification process, after initially registering, Uber drivers are occasionally asked to undergo a security check by taking a "selfie" picture of themselves before they are allowed to continue using their Uber application to verify that the person driving the vehicle is the same individual who originally registered with the application:[2]



Verification Required

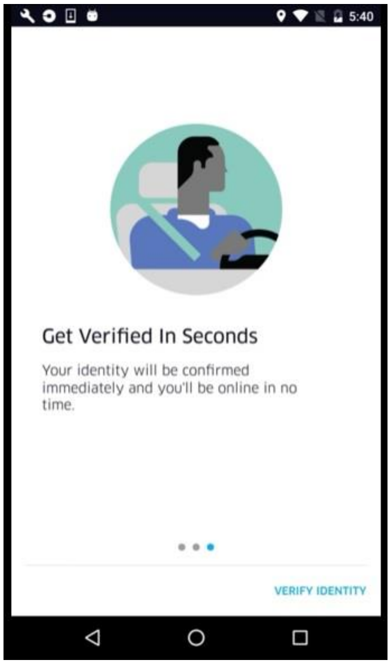
You've randomly been selected to verify your identity. This should take less than a minute.

By proceeding, you agree that Uber or a trusted vendor may collect and process your photos with technology that allows us to verify your identity. More Info



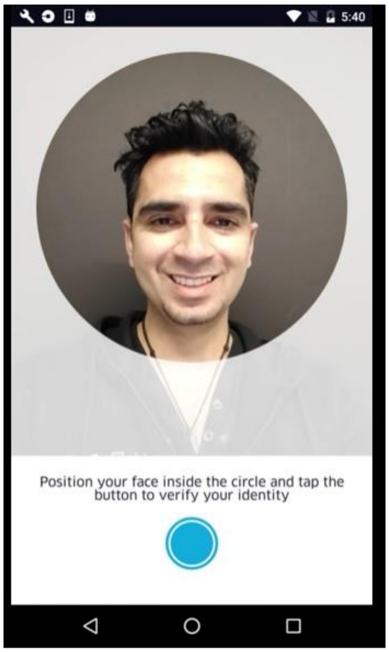
Keep Your Account Secure

We randomly ask partners to verify their identity by taking a photo. This will not replace your profile picture.



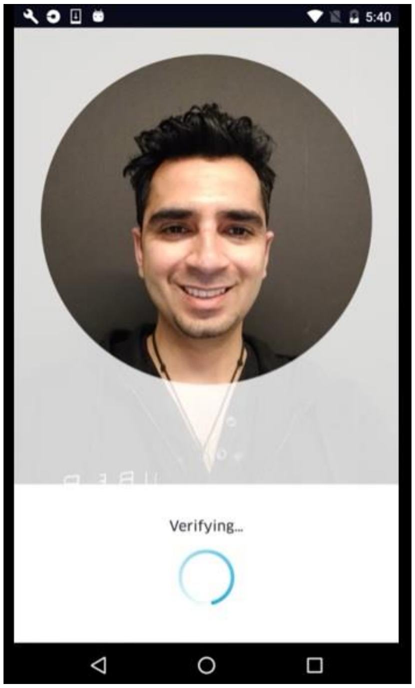
Get Verified In Seconds

Your identity will be confirmed immediately and you'll be online in no time.

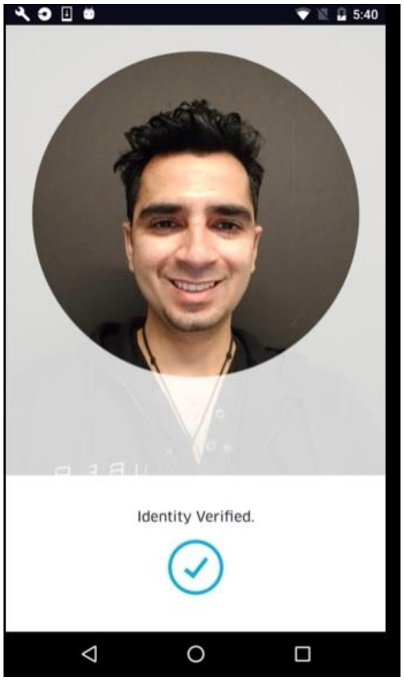


Position your face inside the circle and tap the button to verify your identity

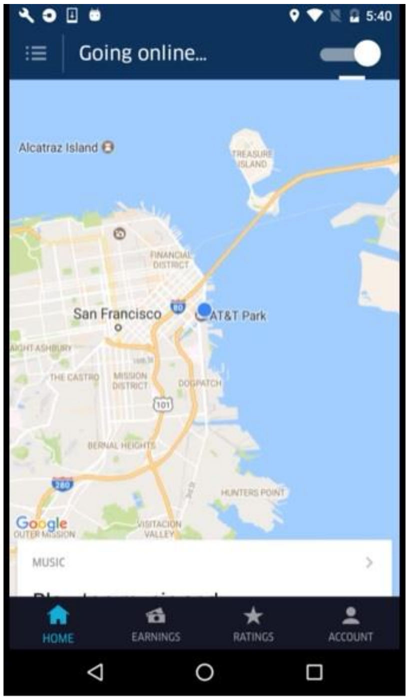
[2] https://eng.uber.com/real-time-id-check/ (last accessed July 29, 2021).



Verifying...



Identity Verified.



Going online...

26. Unbeknownst to the Uber drivers such as Plaintiffs and the other Class members, Uber's "Real Time ID Check" works by taking the driver's picture and providing it to Defendant's Face API software which extracts their facial biometrics to create a geometric template that it then

compares with the geometric template obtained from the original picture taken by the driver when they first enrolled.

27. However, even though Defendant obtained Plaintiffs' and the other Class members' facial biometrics, Defendant failed to obtain proper written consent as required by BIPA to collect their facial biometrics, including from Plaintiffs and the other Class member.

28. Furthermore, Defendant also failed to make publicly available a policy as to Defendant's retention and deletion practices regarding the biometrics in its possession.

29. Defendant also unlawfully profited from the facial biometrics it obtained from Uber drivers, including Plaintiffs and the other Class members, as Defendant was paid by Uber for its use of Defendant's Face API software to verify Uber drivers' facial biometrics through its Real Time ID Check feature.

## <u>FACTS SPECIFIC TO PLAINTIFF EMAD KASHKEESH</u>

30. Plaintiff Emad Kashkeesh was a driver for Uber beginning in 2016, working primarily in Chicago, Illinois. Upon registering as an Uber driver, Plaintiff Kashkeesh, like all other Uber drivers in Illinois, was required to submit a headshot picture to Uber through its mobile application.

31. During Plaintiff Kashkeesh's time as a driver for Uber, on at least one occasion Uber's mobile application required Plaintiff Kashkeesh to take a picture of his face in real time through Uber's "Real Time ID Check" security feature to gain access to Uber's platform and continue driving.

32. Each time Plaintiff Kashkeesh submitted a picture through Uber's Real Time ID Check, the picture was provided to or otherwise transferred to Defendant's Face API software which then extracted Plaintiff Kashkeesh's facial biometric profile to create a geometric template

that was used to confirm that Plaintiff Kashkeesh had the same facial biometrics as identified by Defendant's Face API in prior pictures he had provided to Uber.

33. Plaintiff Kashkeesh, like the thousands of other Illinois Uber drivers who are members of the Class, never provided written consent allowing Defendant to capture, store, or disseminate his facial biometrics.

34. Plaintiff Kashkeesh, like the other members of the Class, was also never informed that Defendant collected and/or possessed his facial biometrics, nor did Defendant make publicly available any policy regarding its practices for the retention or deletion of the biometrics it collects from Uber drivers like Plaintiff Kashkeesh and the other members of the Class.

35. Plaintiff Kashkeesh to this day does not know the whereabouts of his facial biometrics which Defendant obtained from him.

## FACTS SPECIFIC TO PLAINTIFF BEAU ZANCA

36. Beau Zanca was a driver for Uber Eats beginning in 2021, working primarily in Chicago, Illinois. Upon registering as an Uber driver, Plaintiff Zanca, like all other Uber drivers in Illinois, was required to submit a headshot picture to Uber through its mobile application.

37. During Plaintiff Zanca's time as a driver for Uber Eats, on at least one occasion Uber's mobile application required Plaintiff Zanca to take a picture of his face in real time through Uber's "Real Time ID Check" security feature to gain access to Uber's platform and continue making deliveries.

38. Each time Plaintiff Zanca submitted a picture through Uber's Real Time ID Check, the picture was provided to or otherwise transferred to Defendant's Face API software which then extracted Plaintiff Zanca's facial biometric profile to create a geometric template that was used to confirm that he had the same facial biometrics as identified by Defendant's Face API in prior pictures Plaintiff Zanca had provided to Uber.

39. Plaintiff Zanca, like the thousands of other Illinois Uber drivers who are members of the Class, never provided written consent allowing Defendant to capture, store, or disseminate his facial biometrics.

40. Plaintiff Zanca, like the other members of the Class, was also never informed that Defendant collected and/or possessed his facial biometrics, nor did Defendant make publicly available any policy regarding its practices for the retention or deletion of the biometrics it collects from Uber drivers like Plaintiff Zanca and the other members of the Class.

41. Plaintiff Zanca to this day does not know the whereabouts of his facial biometrics which Defendant obtained from him.

## FACTS SPECIFIC TO PLAINTIFF MICHAEL KOMORSKI

42. Plaintiff Michael Komorski was a driver for Uber beginning in 2017, working primarily in Chicago, Illinois. Upon registering as an Uber driver, Plaintiff Komorski, like all other Uber drivers in Illinois, was required to submit a headshot picture to Uber through its mobile application.

43. On multiple occasions during Plaintiff Komorski's time as a driver for Uber, Uber's mobile application required Plaintiff Komorski to take a picture of his face in real time through Uber's "Real Time ID Check" security feature to gain access to Uber's platform and continue driving.

44. Each time Plaintiff Komorski submitted a picture through Uber's Real Time ID Check, the picture was provided to or otherwise transferred to Defendant's Face API software which then extracted Plaintiff Komorski's facial biometric profile to create a geometric template that was used to confirm that he had the same facial biometrics as identified by Defendant's Face API in prior pictures Plaintiff Komorski had provided to Uber.

45. Plaintiff Komorski, like the thousands of other Illinois Uber drivers who are members of the Class, never provided written consent allowing Defendant to capture, store, or disseminate his facial biometrics.

46. Plaintiff Komorski, like the other members of the Class, was also never informed that Defendant collected and/or possessed his facial biometrics, nor did Defendant make publicly available any policy regarding its practices for the retention and deletion of the biometrics it collects from Uber drivers like Plaintiff and the other members of the Class.

47. Plaintiff Komorski to this day does not know the whereabouts of his facial biometrics which Defendant obtained from him.

## **CLASS ALLEGATIONS**

48. Plaintiffs bring this action on behalf of themselves and similarly situated individuals pursuant to Rule 23 of the Federal Rules of Civil Procedure. Plaintiffs seek to represent a Class defined as follows:

> All individuals whose facial biometric identifiers or biometric information were collected, captured, stored, transmitted, disseminated, or otherwise used by Defendant as part of Uber's Real Time ID Check within the state of Illinois any time within the applicable limitations period.

49. Excluded from the Class are any members of the judiciary assigned to preside over this matter; any officer or director of Defendant; and any immediate family member of such officer or director.

50. There are thousands of members of the Class, making the members of the Class so numerous that joinder of all members is impracticable. Although the exact number of members of the Class is currently unknown to Plaintiffs, the members can be easily identified through Defendant's records.

51. Plaintiffs' claims are typical of the claims of the Class they seek to represent, because the basis of Defendant's liability to Plaintiffs and the Class is substantially the same, and because Defendant's conduct has resulted in similar injuries to Plaintiffs and to the Class.

52. There are many questions of law and fact common to the claims of Plaintiffs and the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include, but are not limited to, the following:

a. Whether Defendant collects, captures, or otherwise obtains facial biometric identifiers or biometric information from Illinois residents who are drivers for Uber;

b. Whether Defendant disseminated facial biometrics;

c. Whether Defendant obtained a written release from the Class members before capturing, collecting, or otherwise obtaining their facial biometric identifiers or biometric information;

d. Whether Defendant made publicly available any written policy establishing biometric retention or destruction guidelines;

e. Whether Defendant's conduct violates BIPA;

f. Whether Defendant's BIPA violations are willful or reckless; and

g. Whether Plaintiffs and the Class are entitled to damages and injunctive relief.

53. Absent a class action, most members of the Class would find the cost of litigating their claims to be prohibitively expensive and would thus have no effective remedy. The class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation in that it conserves the resources of the courts and the litigants and promotes consistency and efficiency of adjudication.

54. Plaintiffs will fairly and adequately represent and protect the interests of the other members of the Class they seek to represent. Plaintiffs have retained counsel with substantial

experience in prosecuting complex litigation and class actions. Plaintiffs and their counsel are committed to vigorously prosecuting this action on behalf of the other members of the Class and have the financial resources to do so. Neither Plaintiffs nor their counsel have any interest adverse to those of the other members of the Class.

55. Defendant has acted and failed to act on grounds generally applicable to the Plaintiffs and the other members of the Class, requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the members of the Class and making injunctive or corresponding declaratory relief appropriate for the Class as a whole.

## COUNT I
## Violations of the Illinois Biometric Information Privacy Act, 740 ILCS 14/15(a), *et seq*.
## (On behalf of Plaintiffs and the Class)

56. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

57. Defendant Microsoft is a private entity under BIPA.

58. As discussed above, Plaintiffs and the other Class members have had their "biometric identifiers," namely their facial biometrics, collected and stored, and thus possessed, by Defendant as a result of interacting with Uber's mobile application.

59. Section 15(a) of BIPA requires any entity in possession of biometric identifiers or biometric information to "develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first." 740 ILCS 14/15(a).

60. Though Defendant has come into possession of Plaintiffs' and other Class members' facial biometric identifiers, it has failed to make publicly available any policy addressing its biometric retention and destruction practices.

61. As a result, Defendant has violated Section 15(a) of BIPA.

62. Defendant knew, or was reckless in not knowing, that its Face API software which thousands of Illinois residents interacted with, would be subject to Section 15(a) of BIPA, a statutory provision passed in 2008, yet failed to comply with the statute.

63. BIPA provides for statutory damages of $5,000 for each willful and/or reckless violation of BIPA and, alternatively, damages of $1,000 for each negligent violation of BIPA. 740 ILCS 14/20(1)-(2).

64. Defendant's violations of Section 15(a) of BIPA, which has been in effect since 2008, were knowing and willful, or were at least in reckless disregard of the statutory requirements. Alternatively, Defendant negligently failed to comply with Section 15(a) of BIPA.

65. Accordingly, with respect to Count I, Plaintiffs, individually and on behalf of the proposed Class, pray for the relief set forth below.

## COUNT II
## Violations of the Illinois Biometric Information Privacy Act, 740 ILCS 14/15(b), *et seq*.
## (On behalf of Plaintiffs and the Class)

66. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

67. Defendant Microsoft is a private entity under BIPA.

68. As discussed above, Plaintiffs and the other Class members have had their "biometric identifiers," namely their facial biometrics, collected, captured, and stored by Defendant as a result of interacting with Uber's mobile application.

69. BIPA requires a private entity, such as Defendant, to obtain informed written consent from individuals before acquiring their biometric identifiers or biometric information. Specifically, BIPA makes it unlawful to "collect, capture, purchase, receive through trade, or otherwise obtain a person's or customer's biometric identifiers or biometric information unless [the entity] first: (1) informs the subject . . . in writing that a biometric identifier or biometric information is being collected or stored; (2) informs the subject . . . in writing of the specific purpose and length of for which a biometric identifier or biometric information is being captured, collected, stored, and used; and (3) receives a written release executed by the subject of the biometric identifier or biometric information . . . ." 740 ILCS 14/15(b).

70. Each instance when Plaintiffs and the other Class members interacted with Uber's Real Time ID Check, Defendant captured, collected or otherwise obtained Plaintiffs' and the other Class members' facial biometric identifiers without their written consent and without complying with and, thus, in violation of BIPA.

71. Defendant's practice with respect to capturing, collecting, storing, and using biometrics fails to comply with applicable BIPA requirements:

a. Defendant failed to inform Plaintiffs and the members of the Class in writing that their biometrics were being collected and stored, prior to such collection or storage, as required by 740 ILCS 14/15(b)(1);

b. Defendant failed to inform Plaintiffs and the Class in writing of the specific purpose for which their biometrics were being captured, collected, stored, and used, as required by 740 ILCS 14/15(b)(2);

c. Defendant failed to inform Plaintiffs and the Class in writing the specific length of term their biometrics were being captured, collected, stored, and used, as required by 740 ILCS 14/15(b)(2); and

d. Defendant failed to obtain a written release from Plaintiffs and the other Class members, as required by 740 ILCS 14/15(b)(3).

72. As a result, Defendant has violated Section 15(b) of BIPA.

73. Defendant knew, or was reckless in not knowing, that its Face API software which thousands of Illinois residents interacted with, would be subject to Section 15(b) of BIPA, a statutory provision passed in 2008, yet failed to comply with the statute.

74. BIPA provides for statutory damages of $5,000 for each willful and/or reckless violation of BIPA and, alternatively, damages of $1,000 for each negligent violation of BIPA. 740 ILCS 14/20(1)-(2).

75. Defendant's violations of Section 15(b) of BIPA, a statutory provision that has been in effect since 2008, were knowing and willful, or were at least in reckless disregard of the statutory requirements. Alternatively, Defendant negligently failed to comply with Section 15(b) of BIPA.

76. Accordingly, with respect to Count II, Plaintiffs, individually and on behalf of the proposed Class, pray for the relief set forth below.

## <u>COUNT III</u>
## Violations of the Illinois Biometric Information Privacy Act, 740 ILCS 14/15(c), *et seq*.
## (On behalf of Plaintiffs and the Class)

77. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

78. Defendant Microsoft is a private entity under BIPA.

79. As discussed above, Plaintiffs and the other Class members have had their "biometric identifiers," namely their facial biometrics, collected, captured, and stored by Defendant as a result of interacting with Uber's mobile application.

80. Section 15(c) of BIPA prohibits any private entity in possession of biometrics, such as Defendant, from selling, leasing, trading, or otherwise profiting from such biometrics. 740 ILCS 14/15(d).

81. As alleged herein, Defendant profited from the facial biometrics it obtained from Uber drivers, including Plaintiffs and the other Class members, as Defendant was paid by Uber for its use of Defendant's Face API software to verify Uber drivers' facial biometrics through the Real Time ID Check feature.

82. Accordingly, Defendant has violated Section 15(c) of BIPA.

83. Defendant knew, or was reckless in not knowing, that its Face API Software would be subject to the provisions of Section 15(c) of BIPA, a statutory provision in effect since 2008, yet failed to comply with the statute.

84. BIPA provides for statutory damages of $5,000 for each willful and/or reckless violation of BIPA and, alternatively, damages of $1,000 for each negligent violation of BIPA. 740 ILCS 14/20(1)-(2).

85. Defendant's violations of Section 15(c) of BIPA, a statutory provision that has been in effect since 2008, were knowing and willful, or were at least in reckless disregard of the statutory requirements. Alternatively, Defendant negligently failed to comply with Section 15(c) of BIPA.

86. Accordingly, with respect to Count III, Plaintiffs, individually and on behalf of the proposed Class, pray for the relief set forth below.

## COUNT IV

## Violations of the Illinois Biometric Information Privacy Act, 740 ILCS 14/15(d), *et seq.*

## (On behalf of Plaintiffs and the Class)

87. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

88. Defendant Microsoft is a private entity under BIPA.

89. As discussed above, Plaintiffs and the other Class members have had their "biometric identifiers," namely their facial biometrics, collected, captured, and stored by Defendant as a result of interacting with Uber's mobile application.

90. Section 15(d) of BIPA prohibits any private entity in possession of biometrics, such as Defendant, from disclosing, redisclosing, or otherwise disseminating an individual's biometric identifiers or biometric information without that individual's consent. 740 ILCS 14/15(d).

91. As alleged herein, after Plaintiffs' and other Class members' biometric identifiers were obtained by Defendant through Uber's mobile application and Defendant disclosed or otherwise disseminated their biometrics for identity verification purposes.

92. Defendant never obtained Plaintiffs' or other Class members' consent to disclose or disseminate their biometrics.

93. Accordingly, Defendant has violated Section 15(d) of BIPA.

94. Defendant knew, or was reckless in not knowing, that its biometric dissemination practices would be subject to the provisions of Section 15(d) of BIPA, a statutory provision in effect since 2008, yet failed to comply with the statute.

95. BIPA provides for statutory damages of $5,000 for each willful and/or reckless violation of BIPA and, alternatively, damages of $1,000 for each negligent violation of BIPA. 740 ILCS 14/20(1)-(2).

96. Defendant's violations of Section 15(d) of BIPA, a statutory provision that has been in effect since 2008, were knowing and willful, or were at least in reckless disregard of the statutory requirements. Alternatively, Defendant negligently failed to comply with Section 15(d) of BIPA.

97. Accordingly, with respect to Count IV, Plaintiffs, individually and on behalf of the proposed Class, pray for the relief set forth below.

## PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the proposed Class, respectfully requests that this Court enter an Order:

a. Certifying the Class as defined above, appointing Plaintiffs as class representatives and the undersigned as class counsel;

b. Declaring that Defendant's actions, as set forth herein, violate BIPA;

c. Awarding injunctive and equitable relief as necessary to protect the interests of Plaintiffs and the Class by requiring Defendant to comply with BIPA;

d. Awarding statutory damages of $5,000 for each willful and/or reckless violation of BIPA, pursuant to 740 ILCS 14/20(2);

e. Awarding statutory damages of $1,000 for each negligent violation of BIPA, pursuant to 740 ILCS 14/20(1);

f. Awarding reasonable attorneys' fees, costs, and other litigation expenses, pursuant to 740 ILCS 14/20(3);

g. Awarding pre- and post-judgment interest, as allowable by law; and

h. Awarding such further and other relief as the Court deems just and equitable.

## JURY DEMAND

Plaintiffs request trial by jury of all claims that can be so tried.

Dated: July 30, 2021

Respectfully Submitted,

EMAD KASHKEESH, BEAU ZANCA,
MICHAEL KOMORSKI, individually and
on behalf of similarly situated individuals

By: /s/ Eugene Y. Turin
*One of Plaintiffs' Attorneys*

Eugene Y. Turin
Timothy P. Kingsbury
Andrew T. Heldut
Colin P. Buscarini
MCGUIRE LAW, P.C.
55 W. Wacker Drive, 9th Fl.
Chicago, IL 60601
Tel: (312) 893-7002
eturin@mcgpc.com
tkingsbury@mcgpc.com
aheldut@mcgpc.com
cbuscarini@mcgpc.com

*Attorneys for Plaintiffs and the Putative Class*